*Bull. Soc. Photogr. Imag. Japan.* (2015) Vol. 25 No. 1: 7–11

**Original Paper**

# Palette-Based Image Steganography for High-Capacity Embedding

Shoko Imaizumi* and Kei Ozawa*

**Abstract:** We propose an efficient steganographic scheme for palette-based images that improves the maximum length of the embedded message and does not seriously degrade the image quality in this paper. The proposed scheme embeds a multiple-bit message within the units of a 2 × 2 pixel matrix by assigning a parity to each pixel matrix according to the Euclidean distance. The stego-images created by using our scheme offer a better quality than those by the conventional scheme. Furthermore, the maximum length of the embedded message in our new approach is increased more than twofold compared to that in our previous work. A performance analysis validated our scheme.

**Key words:** Steganography, Information embedding, Palette-based image

## 1. Introduction

Steganography [1] is a practical data hiding technique that is a means of secret communication without drawing attackers' attention. Secret data is imperceptibly embedded into digital multimedia, e.g., images, audio, and video. When the cover medium is an image, the cover image that possesses secret data actually forms a stego-image. The stego-image can be transmitted through open channels without suspicion since the secret data is generally embedded into the cover image without creating noticeable artifacts. The authorized recipient can extract the embedded message from the stego-image, while unexpected users are unaware of the existence of the message behind the stego-image.

Palette-based images, for instance, GIF, PNG, and 8-bits BMP, generally utilize no more than 256 color palette entries (simply called entries hereafter). They are frequently used in digital multimedia and Internet applications. Each pixel in a palette-based image possesses an index value that points to the entry, which is stored in a color palette. Entries specify the RGB colors in the image.

Steganographic schemes for palette-based images embedding data by controlling entries can be classified into two types. One of them changes the colors of the entries in order to embed a message with only slight degradation [2–4]. Wang's scheme [2], for instance, firstly changes two similar colors $i$, $j$ into a new quantized color, and the cover image is generated by this process. We assume that the index of the target pixel is denoted as $x$. If the message bit is 0, then replace $x$ with $i$. Otherwise, replace $x$ with $j$. Thus, the stego-image in this scheme is the same quality as the cover image, which is determined before embedding. The other retains the colors of the entries and may reorder the entries in the palette [5–12]. Liu et al. [5], for instance, proposed a distortion-free data hiding scheme by copying the RGB information of the most frequently used entry to unused entries. Fridrich [6] presented a steganographic scheme for hiding message bits into the parity bit of each close color. The former schemes [2–4] create some new entries in the palette, and remove the same number of entries as the new entries. Thus, the schemes should increase the computational cost of the calculation for adding and removing entries. Our scheme adopts the latter schemes [5–12].

We propose a multiple-bit embedding steganographic scheme for palette-based images in this paper. The proposed scheme enhanced the maximum length of the embedded message by using 2 × 2 pixel matrices, compared to our previous work [8] that uses 4 × 4 pixel matrices, without serious degradation of image quality. Our new scheme also forms better quality stego-images than Tanaka's scheme [7] that expands Fridrich's scheme [6]. The experimental results show that the proposed scheme is efficient.

## 2. Rerated Works

We review two conventional steganographic schemes for palette-based images [6][7], which reorders the entries in the palette, in this section. Our proposed scheme is based on these schemes.

### 2.1 Fridrich's scheme [6]

Fridrich proposed a famous scheme to embed a $Z$-bit message into the pixels of the target image using one-bit parities. This scheme embeds a secret message using the following steps.

**Step 1**: Calculate parities $P_i$ for all entries $E_i$ ($r_i$, $g_i$, $b_i$) in the palette, which is defined as

$$P_i = (r_i + g_i + b_i) \bmod 2, \quad i = 0, 1, \ldots, X-1, \tag{1}$$

Received 4th, September 2014; Accepted 16th, January 2015

*Graduate School of Advanced Integration Science, Chiba University, 1-33 Yayoicho, Inage-ku, Chiba-shi, Chiba 263-8522, Japan

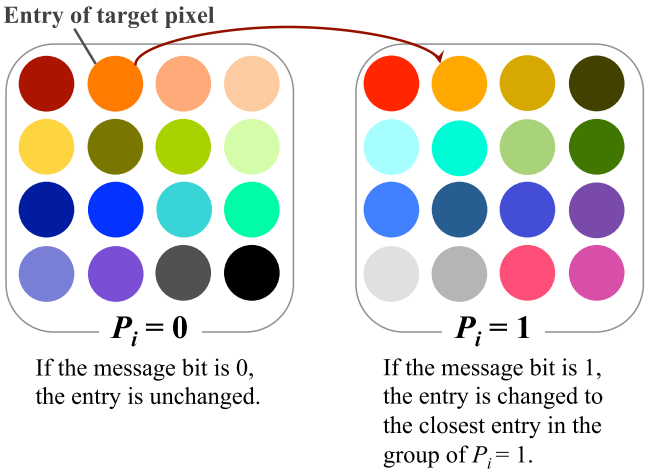



Fig. 1. Embedding message bit into target pixel in Fridrich's scheme [6].

where $X$ is the number of the entries.

**Step 2**: Choose the $z$-th target pixel ($z$ = 1, 2, ..., $Z$) that possesses the entry $E_i$, whose parity bit is $P_i$, in the cover image. Note that if the $z$-th message bit $M_z$ to be embedded is equal to $P_i$, leave the $z$-th pixel unchanged and repeat **Step 2** with $z = z + 1$.

**Step 3**: Find the closest entry $E_{i,\,close}$ to the entry $E_i$ in the group of entries whose parities are equal to $M_z$, by using the Euclidean distance $D_{i,j}$, as shown in Fig. 1. The distance $D_{i,j}$ between two entries $E_i$ ($r_i$, $g_i$, $b_i$) and $E_j$ ($r_j$, $g_j$, $b_j$) is given by

$$D_{i,j} = \sqrt{(\Delta r_{i,j})^2 + (\Delta g_{i,j})^2 + (\Delta b_{i,j})^2}\,, \tag{2}$$

where $\Delta r_{i,j} = |\, r_i - r_j \,|$, $\Delta g_{i,j} = |\, g_i - g_j \,|$, and $\Delta b_{i,j} = |\, b_i - b_j \,|$.

**Step 4**: Replace the entry $E_i$ of the target pixel with the closest entry $E_{i,\,close}$.

**Step 5**: Return to **Step 2** with $z = z + 1$ until $z = Z$.

The message can be easily recovered by collecting the parity bits for the entries of the target pixels according to the location map. Although this scheme can avoid replacing the colors of the target pixels with completely different ones, it can only embed a one-bit message per pixel.

### 2.2 Tanaka's scheme [7]

Tanaka presented an effective steganography that is based on Fridrich's scheme. This scheme can embed a $k$-bit message per pixel without increasing the degradation of the image quality compared to that for Fridrich's scheme. It is because Tanaka's scheme assigns different parities to the entries that are close from each other in the color space. The main contribution of this scheme is assigning a $k$-bit parity to each entry. A parity $P_i$ is assigned to each entry $E_i$ ($i$ = 0, 1, ..., $X - 1$)using the following steps.

**Step 1**: Set the initial entry $E_{i(0)}$, that is

$$E_{i(0)} = \arg\min_i (256^2 r_i + 256^1 g_i + 256^0 b_i). \tag{3}$$

(a) Original (b) Original: expanded (c) Stego: expanded

Fig. 2. Example of result obtained using Tanaka's scheme [7].

**Step 2**: Assign 0 to the parity $P_{i(0)}$ of $E_{i(0)}$.

**Step 3**: Set $x$ = 1.

**Step 4**: Find the next entry $E_{i(x)}$, that is

$$E_{i(x)} = \arg\min_{i \in \alpha} D_{i(x-1),\,i}\,, \tag{4}$$

where $D$ is defined by Eq. (2) and $\alpha$ denotes a set of $i$ in which each entry $E_i$ has not been assigned a parity yet.

**Step 5**: Assign $x$ to the parity $P_{i(x)}$ of $E_{i(x)}$.

**Step 6**: Return to **Step 4** with $x = x + 1$ until $x = 2^k - 1$.

**Step 7**: Find the next entry $E_{i(x)}$, which is given by Eq. (4).

**Step 8**: Find the closest entry $E_{i(x),\mathrm{closest}_p}$ to $E_{i(x)}$ in the set $\alpha_p$ on each parity $p$ ($p$ = 0, 1, ..., $2^k - 1$), which are given by

$$E_{i(x),\mathrm{closest}_p} = \arg\min_{i(y)_p \in \alpha_p} D_{i(x),\,i(y)_p}\,, \tag{5}$$

where $y < x$, and $\alpha_p$ is a set of $i(y)_p$ in which each entry $E_{i(y)_p}$ has already been assigned the parity $p$.

**Step 9**: Assign $z$ ($z$ = 0, 1, ..., $2^k - 1$), that is

$$z = \arg\max_p D_{i(x),\,i(x)_{p,closest}}\,, \tag{6}$$

to the parity $P_{i(x)}$ of $E_{i(x)}$.

**Step 10**: Return to **Step 8** with $x = x + 1$ until $x = X - 1$.

The embedding procedure is the same as that for Fridrich's scheme. When a message is embedded into a cover image as shown in Fig. 2(a), a part of the image, such as that shown in Fig. 2(b), for instance, is degraded like that shown in Fig 2(c). If the entry of the target pixel has no close entries in the palette, the target pixel is changed to a totally different color, and the stego-image is seriously damaged.

## 3. Proposed Scheme

In this section, we present an efficient steganographic scheme for palette-based images that has less degradation than Tanaka's scheme [7]. Our scheme is based on embedding a message into the pixels using multiple-bit parities of their entries. The maximum length of the embedded message in the proposed approach is increased more than twofold compared to that in our previous work [8]. That is because this scheme uses 2 × 2 pixel matrices to inhibit the serious degradation of a stego-image, while our previous scheme uses 3 × 3 pixel matrices.

### 3.1 Reordering Entries

Assume that we embed a $k$-bit message, where $k$ = 1, 2, or 3, into each 2 × 2 pixel matrix. First, we reorder all $X$ entries $E_i$ ($i$ =

Table 1. Reordered palette in proposed scheme.

| Index $I(x)$ | Entry $E_{i(x)}$ |
|---|---|
| 0 | $\arg\min_i (256^2 r_i + 256 g_i + b_i)$ |
| 1 | $\arg\min_{i\in\alpha} D_{0,i}$ |
| 2 | $\arg\min_{i\in\alpha} D_{1,i}$ |
| ... | ... |
| $X$-2 | $\arg\min_{i\in\alpha} D_{X-3,i}$ |
| $X$-1 | $E_i\ (i \in \alpha)$ |

0, 1, ..., $X-1$) in the palette for a cover image using following steps.

**Step 1**: Find the initial entry $E_{i(0)}$ using Eq. (3).
**Step 2**: Assign 0 to the index $I(0)$ of $E_{i(0)}$.
**Step 3**: Find the next entry $E_{i(x)}$ using Eq. (4).
**Step 4**: Assign $x$ to the index $I(x)$ of $E_{i(x)}$.
**Step 5**: Return to **Step 3** with $x = x + 1$ until $x = X - 1$.

The neighboring entries possess similar colors to each other when using the above steps. The reordered palette is formed in the way shown in Table 1.

### 3.2 Embedding Procedure

We divide an embedded message $M$ into $L$ of $k$-bit blocks ($k$ = 1, 2, or 3), which are represented as $M_l$ ($l$ = 1, 2, ..., $L$). The $k$-bit message $M_l$ is embedded into the pixels $t_{l,j}$ ($j$ = 0, 1, 2, 3) in the $l$-th 2 × 2 pixel matrix, which are shown in Fig. 3. The embedding procedure is as follows.

**Step 1**: Choose the $l$-th target matrix with four pixels $t_{l,j}$.
**Step 2**: Calculate the parity $P_l$ for the $l$-th matrix given as

$$P_l = \sum_{j=0}^{3} I_{i,j} \mod 2^k \tag{7}$$

Note that $I_{l,j}$ indicates $I(x)$ ($x$ = 0, 1, ..., or $X-1$).
**Step 3**: Calculate the minimal error $R_l$ between $M_l$ and $P_l$, as shown in Fig. 4.

$$R_l = \begin{cases} \min(P_l - M_l, M_l - P_l + 2^k), & \text{if } M_l < P_l \\ \min(M_l - P_l, P_l - M_l + 2^k), & \text{if } M_l > P_l. \end{cases} \tag{8}$$

If $R_l$ = 0, i.e., $M_l = P_l$, leave the $l$-th matrix unchanged and return to **Step 1** with $l = l + 1$.
**Step 4**: Choose $R_l$ of the pixels $t_{l,j}$ in ascending order corresponding to the Euclidean distance $D_{l,j}$ between the entry $E_{l,j}$ and the neighboring entry $E_{i(x-1)}$ or $E_{i(x+1)}$. The distance $D_{l,j}$ between the two entries is given as

$$D_{l,j} = \begin{cases} D_{i(x),i(x-1)}, & \text{if } R_l = P_l - M_l\ (M_l < P_l) \text{ or } R_l = P_l - M_l + 2^k\ (M_l > P_l) \\ D_{i(x),i(x+1)}, & \text{if } R_l = M_l - P_l\ (M_l > P_l) \text{ or } R_l = M_l - P_l + 2^k\ (M_l < P_l). \end{cases} \tag{9}$$

**Step 5**: Replace $R_l$ of the indices $I_{l,j}$ ( $I_{l,j} = I(x)$) for the pixels $t_{l,j}$, which are chosen by **Step 4**, to $I(x - 1)$ or $I(x + 1)$, respectively.
**Step 6**: Return to **Step 1** with $l = l + 1$ until $l = L$.


Fig. 3. Pixels $t_{l,j}$ in 2 × 2 matrix.

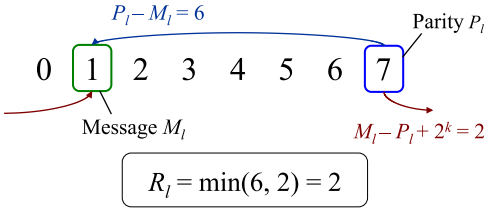



Fig. 4. Decision of minimal error $R_l$ ($k$ = 2, $M_l$ = 1, $P_l$ = 2).

### 3.3 Extracting Procedure

**Step 1**: Choose the $l$-th target matrix with four pixels $t_{l,j}$ according to the location map.
**Step 2**: Calculate the parity $P_l$ for the $l$-th pixel matrix given by Eq. (7).
**Step 3**: Assign $P_l$ to $M_l$.
**Step 4**: Repeat **Steps 1** to **Step 3** with $l = l + 1$ until $l = L$.
**Step 5**: Concatenate all the $k$-bit messages $M_l$ in ascending order of $l$, and read the extracted message $M$.

Note that the recipient has to receive the location map in order to extract the message.

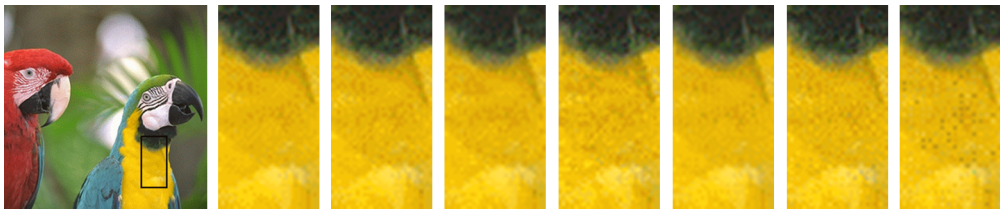
## 4. Experimental Results

We present the experimental results of the proposed scheme and compare them with those of Tanaka's scheme [7]. We performed our experiments on the palette-based images that were 256 × 256 pixels, and embedded a 15,000 × $k$ -bit message, where $k$ = 1, 2, or 3, into each image. This means that the maximum length of the embedded message is 45,000 bit in the proposed scheme, while our previous scheme [8] can embed a 21,000-bit message at the most.

Figs. 5(b) and 6(b) are parts of the original images of Parrots and Pepper from SIDBA, which are enclosed by the squares in Figs. 5(a) and 6(a), respectively. Figs. 5(c), (d), (e) and Figs. 6(c), (d), (e) are the same parts of the stego-images when using the proposed scheme, while Figs. 5(f), (g), (h) and Figs. 6(f), (g), (h) are those using Tanaka's scheme, respectively.

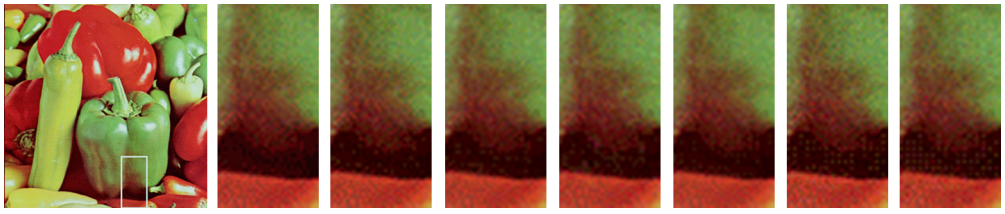
We summarized the evaluation for the stego-images embedded by the proposed scheme using the PSNR values in Fig. 7 to compare them with those for Tanaka's scheme. The maximum difference between those two schemes is 2.54 and the averages in $k$ = 1, 2 and 3 are 1.46, 1.99, and 0.53, respectively. These results for the proposed scheme are superior to those for Tanaka's scheme, especially $k$ = 1 and 2.

Furthermore, we compare the PSNR values between the proposed scheme and our previous work as shown in Fig. 8. The length of the embedded message is 21,000 bits, which is the maximum embedded length that our previous work can embed into a 256 × 256 image. The quality of the stego-images in the proposed scheme is superior to that in our previous work in most of the test images.



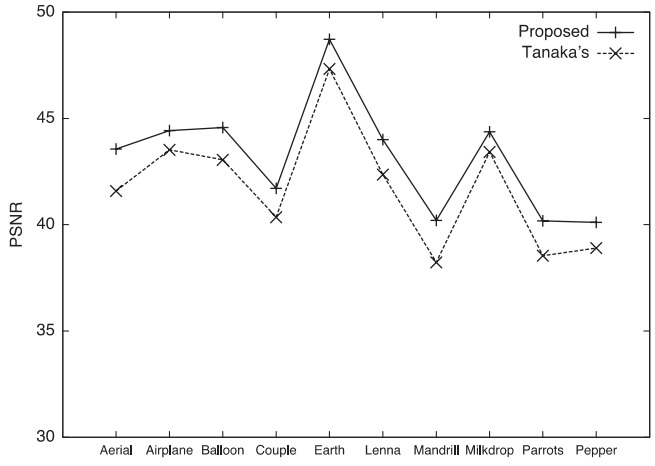
(a) Parrots (b) Original (c) Prop: $k = 1$ (d) Prop: $k = 2$ (e) Prop: $k = 3$ (f) Conv [7]: $k = 1$ (g) Conv [7]: $k = 2$ (h) Conv [7]: $k = 3$

Fig. 5. Comparisons of stego-images between proposed scheme and Tanaka's scheme [7] (Parrots).

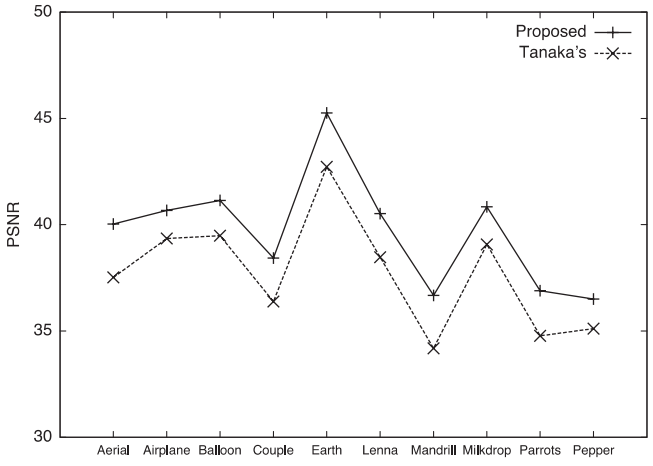


(a) Pepper (b) Original (c) Prop: $k = 1$ (d) Prop: $k = 2$ (e) Prop: $k = 3$ (f) Conv [7]: $k = 1$ (g) Conv [7]: $k = 2$ (h) Conv [7]: $k = 3$

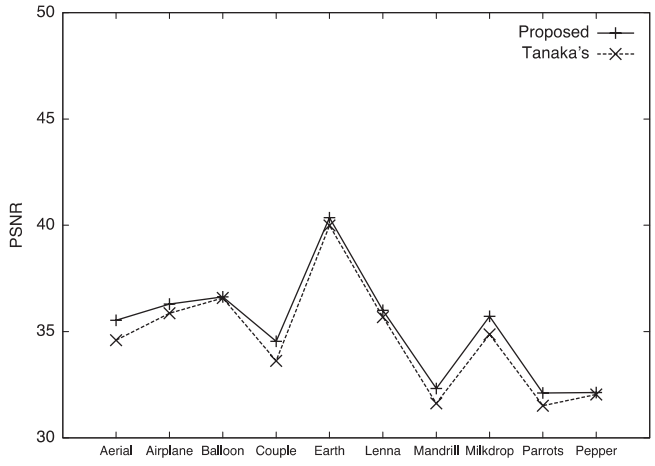
Fig. 6. Comparisons of stego-images between proposed scheme and Tanaka's scheme [7] (Pepper).




(a) $k = 1$




(b) $k = 2$




(c) $k = 3$

Fig. 7. Comparisons of the PSNR values between the proposed scheme and Tanaka's scheme [dB].

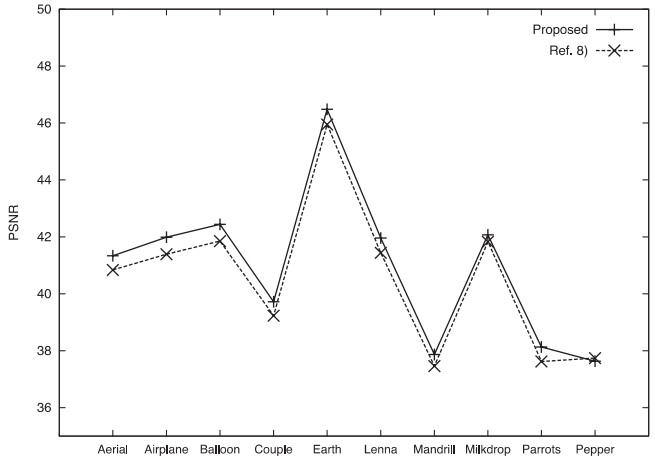



Fig. 8. Comparison of the PSNR values between the proposed scheme and our previous work [8] (The length of the embedded message is 21,000 bits) [dB].

## 5. Summary

We have proposed a new palette-based image steganographic scheme that embeds a multiple-bit message within the units of a 2 × 2 pixel matrix. The proposed scheme improves both of the maximum length of the embedded message and the quality of stego-images, compared to the conventional methods. A performance analysis proved the effectiveness of our scheme. Our future work involves improvement of constructing the matrices to further increase the capacity of the embedded message.

## Acknowledgement

This work was supported by JSPS KAKENHI Grant Number 23800010.

## References

1) A. Cheddad, J. Condell, K. Curran, P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, **90(3)**, 727–752 (2010).
2) X. Wang, Z. Yao, C.-T. Li, "A palette-based image steganographic method using colour quantisation", Proc. IEEE ICIP, **2**, 1090–1093 (2005).
3) M. Niimi, H. Noda, E. Kawaguchi, R. O. Eason, "High capacity and secure digital steganography to palette-based images", Proc. IEEE ICIP, **2**, 917–920 (2002).
4) H. Zhao, H. Wang, M. K. Khan, "Steganalysis for palette-based images using generalized difference image and color correlogram", Signal Processing, **91(11)**, 2595–2605 (2011).
5) H. Liu, Z. Zhang, J. Huang, X. Huang, Y. Q. Shi, "A high capacity distortion-free data hiding algorithm for palette image", Proc. IEEE ISCAS, **2**, 916–919 (2003).
6) J. Fridrich, "A new steganographic method for palette-based images", Proc. IS&T PICS, 285–289 (1999).
7) G. Tanaka, N. Suetake, E. Uchino, "A steganographic method realizing high capacity data embedding for palette-based images", Proc. International Workshop on Smart Info-Media Systems in Asia, 92–95 (2009).
8) S. Imaizumi, K. Ozawa, "Multibit embedding algorithm for steganography of palette-based images", Proc. Pacific-Rim Symposium on Image and Video Technology, **8333** of LNCS, 99–110 (2013).
9) C.-H. Tzeng, Z.-F. Yang, W.-H. Tsai, "Adaptive data hiding in palette images by color ordering and mapping with security protection", IEEE Trans. Commun., **52(5)**, 791–800 (2004).
10) C.-S. Chan, C.-C. Chang, "A color image hiding scheme based on SMVQ and modulo operator", Proc. International Multimedia Modeling Conference, part II, **4352** of LNCS, 461–470 (2007).
11) C.-C. Chang, Y.-H. Chen, Y.-C. Chou, "Reversible data embedding technique for palette images using de-clustering", Proc. International Workshop on Multimedia Content Analysis and Mining, **4577** of LNCS, 130–139 (2007).
12) X. Zhang, S. Wang, Z. Zhou, "Multibit assignment steganography in palette images", IEEE Signal Proc. Lett., **15**, 553–556 (2008).